

Docket No.: 50023-161

He
PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of

Hiroki YAMAUCHI, et al.

Serial No.:

Group Art Unit:

Filed: December 20, 2001

Examiner:

For: DATABASE MANAGEMENT DEVICE, DATABASE MANAGEMENT METHOD
AND STORAGE MEDIUM THEREFOR



**CLAIM OF PRIORITY AND
TRANSMITTAL OF CERTIFIED PRIORITY DOCUMENT**

Commissioner for Patents
Washington, DC 20231

Sir:

In accordance with the provisions of 35 U.S.C. 119, Applicants hereby claim the priority of:

Japanese Patent Application No. 2000-392661, filed December 25, 2000

A Certified copy is submitted herewith.

Respectfully submitted,

MCDERMOTT, WILL & EMERY

Stephen A. Becker
Registration No. 26,527

600 13th Street, N.W.
Washington, DC 20005-3096
(202) 756-8000 SAB:prp
Date: December 20, 2001
Facsimile: (202) 756-8087

50023-161
H. YAMAUCHI et al.
Dec. 20, 2001

日 本 国 特 許 庁
JAPAN PATENT OFFICE

McDermott, Will & Emery

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日
Date of Application:

2000年12月25日

出 願 番 号
Application Number:

特願2000-392661

出 願 人
Applicant(s):

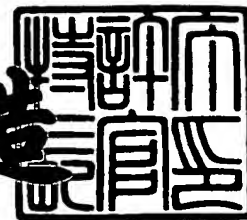
松下電器産業株式会社



2001年 9月13日

特 許 庁 長 官
Commissioner,
Japan Patent Office

及 川 耕 造



出証番号 出証特2001-3084750

【書類名】 特許願

【整理番号】 2022520458

【提出日】 平成12年12月25日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 17/30
G06F 12/547

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 山内 弘貴

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 山口 雅史

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100083172

【弁理士】

【氏名又は名称】 福井 豊明

【手数料の表示】

【予納台帳番号】 009483

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9713946

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 データベース管理装置、管理方法及びその記録媒体

【特許請求の範囲】

【請求項 1】 有効期間を含む必要事項より構成される情報を一データ単位とし、当該データの有効期間が終了するに際して該データに対応する後継データを作成するデータベース管理装置において、

有効期間が終了する所定のデータと、当該所定のデータに対応する後継データとの両方又はいずれか一方に上記データを相互に関連付けた関連情報を追加する関連情報追加手段を具備することを特徴とするデータベース管理装置。

【請求項 2】 さらに、上記所定のデータ又は上記後継データの参照時に、当該データに含まれる上記関連情報を参照して対応するデータを検索する関連情報検索手段を具備する請求項 1 に記載のデータベース管理装置。

【請求項 3】 上記データは、I P S E C (Internet Protocol Security Protocol) 通信に用いられる S A (Security Association) である請求項 2 に記載のデータベース管理装置。

【請求項 4】 有効期間を含む必要事項より構成される情報を一データ単位とし、当該データの有効期間が終了するに際して該データに対応する後継データを作成するデータベース管理装置において、

上記有効期間と、当該有効期間を含むデータの参照情報とを関連付けて記憶すると共に、当該有効期間の終了に際してその旨を通知する有効期間管理手段と、

有効期間管理手段からの通知を受けて、上記データに対して当該有効期間終了に伴う所定の処理を行うデータ制御手段とを備えることを特徴とするデータベース管理装置。

【請求項 5】 上記所定の処理が、上記対応する後継データの作成である請求項 4 に記載のデータベース管理装置。

【請求項 6】 上記所定の処理が、上記有効期間が終了するデータの削除である請求項 4 に記載のデータベース管理装置。

【請求項 7】 上記必要事項より構成される情報が、上記有効期間が終了する前に上記後継データを作成すべき時間情報を含むデータベース管理装置において

更に、上記時間情報と、当該時間情報を含むデータの参照情報とを関連付けて記憶すると共に、当該時間情報にて示された時間の到来を通知する更新管理手段と、

上記更新管理手段からの通知を受けて、上記後継データを作成する上記データ制御手段とを備える請求項4に記載のデータベース管理装置。

【請求項8】 上記有効期間が終了する所定のデータと、当該所定のデータに対応する後継データとの両方又はどちらか一方に上記データを相互に関連付けた関連情報を追加する関連情報追加手段を具備する請求項4又は7に記載のデータベース管理装置。

【請求項9】 上記有効期間の終了を延長する延長期間情報を記憶すると共に、上記有効期間が終了するに際して、当該有効期間が終了するデータの有効期間を上記延長期間情報が示す期間延長する有効期間延長手段を具備する請求項8に記載のデータベース管理装置。

【請求項10】 上記後継データの作成時に、当該後継データの検索順序を、該後継データに対応するデータの前方に位置させる検索順序管理手段を備える請求項4又は7に記載のデータベース管理装置。

【請求項11】 さらに、上記後継データと該後継データに対応するデータの検索頻度を監視する検索頻度監視手段を備え、

上記検索順序管理手段は、上記検索頻度に基づいて上記所定のデータと上記後継データの検索順序を変更する請求項4又は7に記載のデータベース管理装置。

【請求項12】 上記データは、IPSEC(Internet Protocol Security Protocol) 通信に用いられるSA(Security Association)である請求項4に記載のデータベース管理装置。

【請求項13】 有効期間を含む必要事項より構成される情報を一データ単位とし、当該データの有効期間が終了するに際して該データに対応する後継データを作成するデータベース管理方法において、

有効期間が終了する所定のデータと、当該所定のデータに対応する後継データとの両方又はいずれか一方に上記データを相互に関連付けた関連情報を追加する

ステップと

上記所定のデータ又は上記後継データの参照時に、当該データに含まれる上記関連情報を参照して対応するデータを検索するステップとを具備することを特徴とするデータベース管理方法。

【請求項 1 4】 有効期間を含む必要事項より構成される情報を一データ単位とし、当該データの有効期間が終了するに際して該データに対応する後継データを作成するデータベース管理方法において、

上記有効期間と、当該有効期間を含むデータの参照情報とを関連付けて記憶すると共に、当該有効期間の終了に際してその旨を通知するステップと、

有効期間管理手段からの通知を受けて、上記データに対して当該有効期間終了に伴う所定の処理を行うステップとを備えることを特徴とするデータベース管理方法。

【請求項 1 5】 有効期間を含む必要事項より構成される情報を一データ単位とし、当該データの有効期間が終了するに際して該データに対応する後継データをコンピュータにより作成するステップを記録した記録媒体において、

有効期間が終了する所定のデータと、当該所定のデータに対応する後継データとの両方又はどちらか一方に上記データを相互に関連付けた関連情報を追加するステップと

上記所定のデータ又は上記後継データの参照時に、当該データに含まれる上記関連情報を参照して対応するデータを検索するステップとを記録したことを特徴とするコンピュータ読取可能な記録媒体。

【請求項 1 6】 有効期間を含む必要事項より構成される情報を一データ単位とし、当該データの有効期間が終了するに際して該データに対応する後継データをコンピュータにより作成するステップを記録した記録媒体において、

上記有効期間と、当該有効期間を含むデータの参照情報とを関連付けて記憶すると共に、当該有効期間の終了に際してその旨を通知するステップと、

有効期間管理手段からの通知を受けて、上記データに対して当該有効期間終了に伴う所定の処理を行うステップとを記録したことを特徴とするコンピュータ読取可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、データベース管理装置、管理方法及びその記録媒体に係り、詳しくは、データが有効期間を持つデータベースのデータベース管理装置、管理方法及びその記録媒体に関するものである。

【0002】

【従来の技術】

近年、TCP/IPプロトコルを用いたインターネットは、研究教育用ネットワークとしての役割のみならず、インターネットあるいは企業間のイントラネットを介した電子メールの交換や、これらを利用した電子商取引や電子決済にも利用されており、社会と個人のコミュニケーション用ネットワークとしての役割を担う情報通信基盤となっている。

【0003】

しかし、元来インターネットには通信中の情報の秘匿化や改ざんを防止する機能がないため、容易に通信中の情報を盗聴、改ざんすることができた。従って、特に重要な情報を含む通信には専用線並のセキュリティの確保が重要である。

【0004】

上述したようなセキュリティを確保する技術として、例えばインターネットのような広域ネットワークを仮想私設網とするVPN(Virtual Private Network)技術等のセキュリティ通信技術が注目されている。VPNを実現するセキュリティ通信のための接続手順としてトンネリングプロトコルがあり、L2F(Layer 2 Forwarding)、PPTP(Point-to-Point Tunneling Protocol)、L2TP(Layer 2 Tunneling Protocol)、ATMP(Ascend Tunnel Management Protocol)、BayDVSBayStream Dial VPN Service)、IPSEC(Internet Protocol Security Protocol)等が標準化されている。上記セキュリティ通信のためのプロトコルを使用することにより、第3者が通信を盗聴しうる上記広域ネットワークにおいて通信のセキュリティを確保することが可能となる。

【0005】

このようなセキュリティ通信技術のうち、上記 I P S E C は、ネットワーク層（O S I 参照モデル (Open System Interconnection reference model) 第 3 層）で認証、暗号化を行うセキュリティプロトコルであり、インターネット技術の標準化機構である I E T F （Internet Engineering Task Force ）によって標準化されている。その標準化の過程としては、1 9 9 5 年 8 月に I P プロトコルにさまざまなセキュリティ機能を付加した I P S E C プロトコルバージョン 1 が標準化され、さらに 1 9 9 8 年 1 1 月には I P S E C プロトコルバージョン 1 に改訂や機能の拡張を施した I P S E C プロトコルバージョン 2 と暗号認証鍵交換用 I K E プロトコルが標準化された。

【 0 0 0 6 】

上記 I P S E C 機能を搭載したコンピュータや、ネットワーク接続装置であるルータ等を介してインターネットに接続することにより、上記 V P N を構築することが可能である。即ち、ユーザはネットワークの種類を意識することなく、安全にインターネットを利用することができる。尚、I P S E C を利用した通信を行うにあたっては、どのような認証アルゴリズムや暗号化アルゴリズムを使用するか、あるいはどのような暗号化鍵を使用のかなどを、事前に送信側と受信側の I P S E C 機能を搭載したコンピュータ、または、ネットワーク接続装置間で整合を取っておく必要がある。この認証、暗号化アルゴリズムの整合をとるための相互通信を、セキュリティ通信のための接続と呼ぶ。

【 0 0 0 7 】

I P S E C においては、この接続は S A （Security Association）によって実現されている。上記 S A は認証とセキュアメッセージ交換の機能を提供する基本的な枠組であり、その通信のセキュリティのいくつかの側面を定義する。

【 0 0 0 8 】

以下に、図 9、図 1 0、図 1 1、図 1 2 を参照しながら、従来の、セキュリティ通信として I P S E C を用いた通信方法について説明する。又、ここに通信端末とは、ネットワーク接続装置及びコンピュータを含む。

【 0 0 0 9 】

図 9 は、従来のセキュリティ通信として I P S E C 機能を搭載したルータを使

用してVPNネットワークを構成したネットワークシステムの概略図、図10は、上記IPSEC機能を搭載したネットワーク接続装置間でのセキュリティ通信の接続手順を表した図、図11は、従来技術におけるIPSECの処理方針を決めるデータベースであるSPD (Security Policy Database) の例、図12は、従来技術におけるSAデータベースであるSAD (Security Association Database) の例である。ここに、SPDとはセキュリティポリシーを構成するデータベースである。又、セキュリティポリシーとは、セキュリティを確保されたシステムへのアクセス規制のことであり、一般にセキュリティ要件、セキュリティ上のリスク、及びセキュリティの測定手段が含まれる。通信端末間のセキュリティを確保するシステムにおいては、セキュリティを適用する相手先通信端末を区別する情報、セキュリティを適用するかどうかの情報等を備える。尚、IPSECにおいては、セキュリティポリシーは上記SPDに記述され、該SPDには送信先通信端末のIPアドレス、IPSEC処理の有無、認証、暗号化アルゴリズム等の内容を記述した上記SAが格納されるメモリ上のアドレスの参照情報を備える。

【0010】

図9において、コンピュータ901はLAN907 (Local Area Network)で他のコンピュータ905及びネットワーク接続装置902と接続されており、ネットワーク接続装置902を経由して、外部のインターネット909やイントラネット等のWANに接続されている。このインターネット909には他のネットワーク接続装置903を介してコンピュータ904、906が接続されるLAN908が接続されている。ここで、上記ネットワーク接続装置902、903は、ルータ、ゲートウェイ、プロキシサーバ等のファイアウォールやVPN専用装置等である。尚、コンピュータ901他は、パーソナルコンピュータ、ワークステーション、サーバ、ノート型パソコン、IP電話、IPテレビ電話、IP携帯電話等の通信機能をもつ端末であればよい。

【0011】

ここでは上記ネットワーク接続装置902、903にIPSEC機能を搭載し、ネットワーク接続装置902、903間でIPSECによる通信を行うものと

して説明する。また、上記コンピュータ 9 0 1 及び 9 0 4 に IPSEC 機能を搭載し、上記コンピュータ 9 0 1、9 0 4 間で IPSEC による通信を行うことも可能である。さらに、同様に IPSEC 機能を搭載した、コンピュータ 9 0 1 と IPSEC 機能を搭載しているネットワーク接続装置 9 0 3 間で IPSEC による通信を行うことも可能である。

【 0 0 1 2 】

さて、コンピュータ 9 0 1 がインターネット 9 0 9 を介してコンピュータ 9 0 4 にデータを送信する場合には、予め上記ネットワーク接続装置 9 0 2、9 0 3 間において上記セキュリティ通信のための接続を行う必要がある。以下に該セキュリティ通信のための接続について説明する。

【 0 0 1 3 】

IPSEC 通信を始めるにあたり、まず、IPSEC の暗号鍵交換のためのプロトコルである IKE (Internet Key Exchange) が用いられる。該 IKE を使用した通信は、IKE フェーズ 1 と IKE フェーズ 2 とに分けて説明することができ、上記ネットワーク接続装置 9 0 2、9 0 3 間で行われる。尚、IKE による自動鍵交換を行わず、手動で秘密鍵の交換を行ってもよい。

【 0 0 1 4 】

上記 IKE フェーズ 1 (図 1 0 : S 1 0 0 1) では、IKE 自身が安全に通信を行うために、互いに利用可能な SA (Security Association) を確立するための情報を交換する。ここで SA とは、例えば、認証アルゴリズムや認証パラメータ、暗号化アルゴリズムや暗号化パラメータ等を含む一連の定義情報群である。

【 0 0 1 5 】

次に、IKE フェーズ 2 (図 1 0 : S 1 0 0 2) では、前記 IKE フェーズ 1 にて確立した上記 SA を用いて、IPSEC 通信用の SA に関する情報を交換する。ここで、IPSEC 通信用の SA の一例について図 1 2 に示す。図 1 2 は、複数の上記 SA である、SA 1 (1 2 0 2) ~ SAM (1 2 0 4) を含む SAD 1 2 0 1 であり、さらに各 SA には送信ホストアドレス 1 2 0 5、受信ホストアドレス 1 2 0 6、プロトコル 1 2 0 7、当該 SA のインデックス情報である SPI 1 2 0 8 (Security Parameters Index)、登録時刻 1 2 0 9、有効期間 1 2

1 0、更新待ち期間 1 2 1 1、認証アルゴリズム 1 2 1 2、認証鍵 1 2 1 3、暗号化アルゴリズム 1 2 1 4、暗号化鍵 1 2 1 5 等が含まれる。

【 0 0 1 6 】

上記送信ホストアドレス 1 2 0 5 には送信元 IP アドレス、送信元ポート番号が、上記受信ホストアドレス 1 2 0 6 には送信先 IP アドレス、送信先ポート番号が、プロトコル 1 2 0 7 にはプロトコル番号等が含まれる。又、上記 SPI 1 2 0 8 には擬似乱数等が用いられ、当該 SA を特定可能となっている。

【 0 0 1 7 】

さらに、登録時刻 1 2 0 9 には当該 SA を登録した時刻が、有効期間 1 2 1 0 には当該 SA の有効期間が、更新待ち期間 1 2 1 1 には当該 SA の更新迄の期間がそれぞれ格納されているが詳細は後述する。

【 0 0 1 8 】

さらに、認証アルゴリズム 1 2 1 2 には例えば HMAC - MD 5 - 9 6 といった認証アルゴリズムが、暗号化アルゴリズム 1 2 1 4 には例えば DES - CBC といった暗号化アルゴリズムの種別が格納され、認証鍵 1 2 1 3 及び暗号化鍵 1 2 1 5 はそれぞれの認証、暗号化（復号化）に必要な鍵が格納される。

【 0 0 1 9 】

上記 IKE フェーズ 2（1 0 0 2）で行われる IP SEC 通信用の SA に関する情報の交換は、具体的には、ネットワーク接続装置 9 0 2 がネットワーク接続装置 9 0 3 に対し、IP SEC 通信に使用する上記 SA の構成の候補を送信し、該ネットワーク接続装置 9 0 3 は上記候補の中から受け入れ可能な SA を返信するものである。ここで、上記 SA の構成の候補は、上記ネットワーク接続装置 9 0 2 のデータ記憶部に予め記憶されている認証アルゴリズム、暗号化アルゴリズム等を用いて構成される。上記ネットワーク接続装置 9 0 2 がどのような認証アルゴリズム、暗号化アルゴリズムを搭載しているかは、ネットワーク接続装置により異なる。また、予め上記ネットワーク接続装置 9 0 2 が提案する SA を決めておくことも可能である。

【 0 0 2 0 】

上記 SA の返信処理により、IP SEC 通信に使用される SA が確立される。

上記確立されたIPSEC通信に使用されるSAの情報は、図12に示すSAD 1201及び、図11に示すSPD1101に格納される。該SPD1101の構成は以下の例に示される。即ち、受信アドレス1102、IPSEC処理の有無1103、上記SAD1201における各SAの位置を示すアドレスポインタ1104、及び上記受信ホストアドレス1102にデータを送信する場合に、IPSECパケットを送信すべき先の通信端末のIPアドレス1105である。ここで、上記IPアドレス1105は、具体的にはネットワーク接続装置903のIPアドレスとなる。又、送信先の通信端末がIPSEC機能を搭載している場合、上記IPアドレス1102が上記IPアドレス1105と同一となる。さらに、上記受信ホストアドレス1102及びIPアドレス1105は範囲指定が可能である。範囲指定とは、具体的にはIPアドレスを用いて例えば”192.168.1.1~192.168.1.100”という指定を指し、上記範囲指定により1つの指定で例えば200台の通信端末へのデータの送信を指定することが出来る。尚、上記SAは片方向で1つ設定されるので、双方通信の場合は独立したSAがネットワーク接続装置902、903にそれぞれ設定されることになる。

【0021】

上記IPSEC通信に使用されるSAが確立された後、送信側（元）のコンピュータ901から上記コンピュータ904に送信されるデータは、該コンピュータ901にてIPヘッダを付加され、IPパケットとしてLAN907を介してネットワーク接続装置902に送られる。該ネットワーク接続装置902は、後述するIPSEC処理を行うことにより上記IPパケットをIPSECパケット1003として、上記ネットワーク接続装置903に送信する。上記IPSECパケット1003を受信した上記ネットワーク接続装置903は、同じく後述するIPSEC処理にて上記IPSECパケット1003をIPパケットに戻し、上記LAN908を介して上記コンピュータ904に送信する。即ち、上記インターネット909を介して接続される上記ネットワーク接続装置902、903間では、送信側のコンピュータ901から上記コンピュータ904に送信されるデータはIPSECによりセキュリティが確保されるに至る。

【 0 0 2 2 】

続いて、図 9、図 1 3、図 1 4 を用いて上記ネットワーク接続装置 9 0 2 及び 9 0 3 における IP SEC 処理の詳細を説明する。但し、機器構成や採用する方法によって様々な処理が行われるため、ここではその一例のみを示す。ここに図 1 3 は、送信側ネットワーク接続装置における IP SEC 処理のフローチャート、図 1 4 は、受信側ネットワーク接続装置における IP SEC 処理のフローチャートである。尚、後述する SPD、SAD はそれぞれのネットワーク接続装置内のデータ記憶部に記憶されている。ここで、図 1 3、1 4 における S はステップを意味する。

【 0 0 2 3 】

上記ネットワーク接続装置 9 0 2 では、送信側のコンピュータ 9 0 1 より送信された IP パケットを受信すると、まずその受信ホストアドレスを読み出す（図 1 3：S 1 3 0 1）。つづいて該受信ホストアドレスを基に上記ネットワーク接続装置 9 0 2 に格納される上記 SPD 1 1 0 1 の受信ホストアドレス 1 1 0 2 を検索し、対応する IP SEC パケットを送信すべき先の通信端末の IP アドレス 1 1 0 5、IP SEC 処理の有無 1 1 0 3 及び SA の位置を示すアドレスポインタ 1 1 0 4 を読み出す（図 1 3：S 1 3 0 2）。

【 0 0 2 4 】

ここで、IP SEC 処理を行わない設定、即ち IP SEC 処理の有無 1 1 0 3 が”無”の場合、上記受信した IP パケットをそのまま上記ネットワーク接続装置 9 0 3 に送信する（図 1 3：S 1 3 0 3 の No）。

【 0 0 2 5 】

IP SEC 処理を行う設定、即ち IP SEC 処理の有無 1 1 0 3 が”有”の場合、更に上記 SA の位置を示すアドレスポインタ 1 1 0 4 を用いて上記 SAD 1 2 0 1 を検索し、該当する SA の内容を読み出す（図 1 3：S 1 3 0 3 の Yes → S 1 3 0 5）。該 SA は、上記 IKE フェーズ 2（図 1 0：S 1 0 0 2）で確立された SA である。次に、上記ネットワーク接続装置 9 0 2 は、上記 SA の内容に従い、例えば認証アルゴリズムとして HMAC-MD5-96 等を、暗号化アルゴリズムとして DES-CBC 等を用いて上記 IP パケットから認証／暗号

化データを作成する（図13：S1305）。さらに、上記ネットワーク接続装置902は、上記認証／暗号化データに、認証ヘッダAH(Authentication Header) または認証／暗号化ヘッダESP(Encapsulation Security Payload)ヘッダを追加し、IPSEC処理を施したIPパケット（IPSECパケット1003）とする（図13：S1306）。

【0026】

ここで、上記AH及びESPには上記IKEフェーズ2で確立したSAを構成する上記SPI1208が含まれる。続いて上記IPSECパケット1003は、インターネット909を介して上記SPD1101のIPアドレス1105が示す上記ネットワーク接続装置903に送信される。

【0027】

次に、上記ネットワーク接続装置903は、受信したIPパケットがIPSECパケットであるかを判別する（図14：S1401）。

【0028】

ここで、IPSECパケットでない場合、上記IPパケットはそのままLAN908を介してコンピュータ904に送信される（図14：S1401のNo）。

【0029】

受信したIPパケットが、IPSECパケットである場合、以下の処理を行う（図14：S1401のYes）。即ち、まず上記IPSECパケット内の上記AHやESPヘッダを調べ、該AHやESPヘッダに含まれるSPIを読み出す（図14：S1402）。次に、上記ネットワーク接続装置903に格納されるSADを上記SPIを用いて検索し、上記SPIに該当する、上記IKEフェーズ2で確立したSAの内容を読み出す（図14：S1403）。これにより、上述したIKEフェーズ2で確立した該当SAが読み出されることになる。ここで、S1402にて該当SPIが無い場合はユーザにその旨を表示して処理を終了する（図示せず）。

【0030】

さらに、上記ネットワーク接続装置903は、上記読み出したSAで指定され

た認証／暗号化アルゴリズム等を用いて、上記IPSECパケットの認証／暗号化データを認証／復号化する（図14：S1404）。又、必要に応じて上記SAのアドレス1104を用いてSPD1101を検索し、送信（元）ホストのIPアドレス及び、IPSEC処理の有無を確認し、元のIPパケットを生成する（図14：S1405→1406）。続いて上記ネットワーク接続装置903は生成した上記IPパケットをコンピュータ904に送信する。

【0031】

以上により、上記認証／復号化された上記IPSECパケットの認証／暗号化データは、IPパケットとしてLAN908を介してコンピュータ904に送信される。即ち、上記ネットワーク接続装置902、903間では、送信側のコンピュータ901から上記コンピュータ904に送信されるデータはIPSECにてセキュリティが確保される。

【0032】

以上がIPSECについての詳細な処理内容であるが、上記処理に加えて、より一層秘匿性の高い通信を実現するために、以下のような処理が行われる。即ち、上記SA1202～1204に「ライフタイム」と呼ばれる有効期間を設けるものである。

【0033】

例えば所定の通信端末と長時間の通信を行う場合には、第3者に通信中の情報を盗聴し、解析する時間を与えてしまい、即ち情報漏洩の可能性が高くなってしまう。このようなケースでは、上記SAに有効期間を設け、所定の時間間隔を持って再度新たなSAを確立することで秘匿性を高めるのである。

【0034】

即ち、図15に示すように、SA1（1501）は、所定の時間（例えば8時間）の有効期間を有する。当該有効期間の情報は、図12に示した有効期間1210に格納されている。また、上記SA1（1501）が確立（作成、登録）された時刻1502が登録時刻1209に格納されている。上記登録時刻1209と有効期間1210により、SA1（1501）が通信に利用される最終時刻1503が決定される。即ち、上記SA1（1501）の有効期間が過ぎると次に

例えば S A 5 (1 5 0 4) が対応する通信端末との通信に利用されることになる。

【 0 0 3 5 】

但し、上記 S A 5 (1 5 0 4) の確立には、上述したような I K E を用いた複雑な手順が必要となるために、多少の時間 1 5 0 5 を要する。よって、上記更新待ち期間 1 2 1 1 に、例えば最終時刻 1 5 0 3 からの時間 1 5 0 6 や、S A 1 (1 5 0 1) 確立時からの時間 1 5 0 7 等を格納することにより、当該更新待ち期間 1 2 1 1 が示す時刻 1 5 0 8 より S A 5 (1 5 0 4) 確立の為の処理を開始している。

【 0 0 3 6 】

尚、新たな S A 5 (1 5 0 4) が確立された後は、古い S A 1 (1 5 0 1) は有効期間終了時刻の到来をもって上記 S A D から削除されるに至る。

【 0 0 3 7 】

【発明が解決しようとする課題】

上述したように、例えば上記 I P S E C を用いることにより、秘匿性の高い通信が実現できるわけである。しかしながら、上述した処理、特に図 1 4 の S 1 4 0 3 に示した S A を検索する処理は基本的にパケットの送受信毎に行われる。従来では、I P S E C 等におけるボトルネック処理は、暗号化／復号化処理と認証処理であったが、近年、暗号／復号、認証処理のハードウェア化が進行しており、そのボトルネックが解消される方向にある。そのような場合、次に問題となるボトルネック処理としては、上記 S A D の検索処理が挙げられる。特に、ネットワークの通信量が増大し、各端末のパケット処理量が増加すると、この影響が顕著に現れる。さらに、コネクションを集群する基幹ルータなどでは、その影響は特に深刻な問題である。

【 0 0 3 8 】

さらに上記 S A の有効期間は、当該 S A に対応するパケットの、入出力時における S A 検索でのみ検査される。このため、パケットの入出力が中断している期間に、上記 S A の有効期間が過ぎている場合には、それらの時間を検知する方法がない。従って、通信を一時中断している間に S A の有効期間が終了していると

、通信の再開時にまず送受信端で S A の確立をしなければならず、通信が迅速に再開できないといった問題がある。

【 0 0 3 9 】

また、I P S E C プロトコルを用いて長時間のリアルタイム映像通信を行う場合には、通信中に S A の有効期間が過ぎることがあり、当該通信途中に上記 I K E プロトコルで新たな S A を確立した後に新 S A を有効化する場合がある。しかしながら、例えばインターネットのようなネットワークでは、不特定の通信経路が利用されるため、パケットの到着順序が保証されるものではない。従って、受信端末の S A は新 S A になっているのにもかかわらず、旧 S A を適用したパケットが受信端末により受信されるといった状態が発生し得る。

【 0 0 4 0 】

このような状態が発生した場合、上記 S A D 内の新 S A と旧 S A との検索時間の差により、受信した映像にブランクや乱れが生じる。

【 0 0 4 1 】

さらに、有効期間の終了間際に、パケットが送信端から出力された場合には、受信端末にパケットが届く時間には S A の有効期間が終了しており、そのパケットは破棄されてしまうといった問題も生じる。

【 0 0 4 2 】

従って本発明は、有効期間を有するデータベースの管理装置、管理方法及びその記録媒体において、当該データベース内の検索対象となるデータを短時間に検索すると共に、有効期間の終了するデータと当該データの後継データとの切換をスムーズに行うデータベース管理装置、管理方法及びその記録媒体を提供することを目的とするものである。

【 0 0 4 3 】

【課題を解決するための手段】

本発明は、上記目的を達成するために以下の手段を備える。

【 0 0 4 4 】

すなわち、有効期間を含む必要事項より構成される情報を一データ単位とし、当該データの有効期間が終了するに際して該データに対応する後継データを作成

するデータベース管理装置を前提としている。ここで、関連情報追加手段は、有効期間が終了する所定のデータと、これに対応する後継データとの両方又はどちらか一方に関連情報を追加する。

【 0 0 4 5 】

以上により、一方のデータが検索された場合に、関連する他方のデータを瞬時に読み出すことが可能になる。従って、目的とするデータを検索する速度を高めるとともに、データベース管理装置の負荷を下げることができる。

【 0 0 4 6 】

尚、関連情報検索手段が、所定のデータ又は後継データの参照時に、当該データに含まれる上記関連情報を参照して対応するデータを検索する。

【 0 0 4 7 】

又、有効期間管理手段が、有効期間と、当該有効期間を含むデータの参照情報とを関連付けて記憶すると共に、有効期間の終了に際してその旨を通知し、通知を受けた、データ制御手段が上記データに対して当該有効期間終了に伴う所定の処理を行う構成がある。尚、所定の処理が、上記対応する後継データの作成や、上記有効期間が終了するデータの削除である構成がある。

【 0 0 4 8 】

この構成では、データの作成、登録や削除等、必要な処理を確実に行うことができる。上記必要な処理を確実に行うことにより、不要なデータを放置することによる検索速度の低下や記憶領域の無駄を防ぐことが可能となる。

【 0 0 4 9 】

さらに、上記情報が、上記有効期間が終了する前に上記後継データを作成すべき時間情報を含むに際して、時間情報と、当該時間情報を含むデータの参照情報とを関連付けて記憶すると共に、当該時間情報にて示された時間の到来を通知する更新管理手段と、この通知を受けて、後継データを作成する構成がある。尚、この構成において、有効期間が終了する所定のデータと、当該所定のデータに対応する後継データとの両方又はどちらか一方に上記データを相互に関連付けた関連情報を追加する関連情報追加手段を備えてもよい。

【 0 0 5 0 】

更新開始時刻を正確に管理することで、確実に後継データを作成、登録することが可能になる。また、更新待ち期間に十分な余裕を持たすことにより、データと後継データの何れかが常時有効な状態で存在することになり、データの作成、登録のための通信の遅延を確実に無くすることができる。

【 0 0 5 1 】

又、有効期間の終了を延長する延長期間情報を記憶すると共に、上記有効期間が終了するに際して、当該有効期間が終了するデータの有効期間を上記延長期間情報が示す期間延長する有効期間延長手段を具備する構成や、後継データの作成時に、後継データの検索順序を、該後継データに対応するデータの前方に位置させる検索順序管理手段を備える構成もある。

【 0 0 5 2 】

有効期間延長手段を設けることで、本来破棄されるデータ（パケット）を破棄することなく活用することができる。

【 0 0 5 3 】

さらに、上記後継データと該後継データに対応するデータの検索頻度を監視する検索頻度監視手段を備え、検索順序管理手段が、検索頻度に基づいて所定のデータと後継データの検索順序を変更する構成がある。

【 0 0 5 4 】

この構成では、後継データと当該後継データに対応するデータがどちらも検索される期間において、2つのデータのうち検索頻度が高いデータを検索時間の短い検索順序に設定することで、検索頻度の高いデータを短時間で検索することが可能になる。尚、上記データは、I P S E C (Internet Protocol Security Protocol) 通信に用いられる S A (Security Association) としてもよい。

【 0 0 5 5 】

【発明の実施の形態】

以下、添付図面を参照して、本発明の実施の形態につき説明し、本発明の理解に供する。尚、以下の実施の形態は、本発明を具体化した一例であって、本発明の技術的範囲を限定する性格のものではない。

【 0 0 5 6 】

〔実施の形態 1〕

まず、図 1、図 2、図 9 を用いて本実施の形態 1 におけるデータベース管理装置の構成の概略を説明する。尚、上記データベース管理装置 1 0 1 は、図 9 に示したネットワーク接続装置 9 0 2、9 0 3 やコンピュータ 9 0 1 であって、例えば I P S E C 機能を実装する端末内に設けられる。ネットワークの構成においては、図 9 における従来技術と同様の構成を用いて説明する。

【0 0 5 7】

上記ネットワーク接続装置 9 0 2 及び 9 0 3 は、一般的に図 2 に示すような構成を有する。即ち、処理部 2 0 1、一時データ記憶部 2 0 2、データ記憶部 2 0 3、システム制御部 2 0 4、ネットワーク制御部 2 0 6、回線制御部 2 0 7 が内部バス或いはスイッチ 2 0 5 にてそれぞれ接続されている。また、上記ネットワーク制御部 2 0 6 は例えば上記 L A N 9 0 7 に、上記回線制御部 2 0 7 はインターネット 9 0 9 とそれぞれ接続されている。尚、本実施の形態 1 ではネットワーク接続装置 9 0 2 及び 9 0 3 は、ネットワーク制御部 2 0 6 と回線制御部 2 0 7 を 1 個ずつ具備した構成であるが、ネットワーク制御部 2 0 6 のみが複数個ある構成でも構わない。

【0 0 5 8】

従来技術にて示した S P D、S A D は、フラッシュメモリ、ハードディスク、ROM 等の不揮発性メモリで構成された上記データ記憶部 2 0 3 に格納される。上記処理部 2 0 1 は、上記ネットワーク接続装置 9 0 2 の電源投入時に上記データ記憶部 2 0 3 からシステム制御部 2 0 4 を経由して、上記 S P D、S A D を読み出し、D R A M、S R A M 等の揮発メモリで構成される上記一時データ記憶部 2 0 2 に格納するかあるいは、必要なときに読み出し、一時データ記憶部 2 0 2 に格納する。又、上記 S P D、S A D の更新は、上記データ記憶部 2 0 3 及び、一時データ記憶部 2 0 2 に格納されている S P D、S A D に対して行なわれる。

【0 0 5 9】

即ち、図 1 に示すデータベース管理装置 1 0 1 は、上記処理部 2 0 1 にて実行され、例えばソフトウェアやハードウェアとして提供される。また、S A D 1 0 2 は、上記データ記憶部 2 0 3、一時データ記憶部 2 0 2 等に記憶されている。

従って、SADシステム103は、上記処理部201、データ記憶部203及び／又は一時データ記憶部202により構成される。

【0060】

尚、従来技術にて説明したように、LAN907或いはインターネット909からそれぞれネットワーク制御部206、回線制御部207を経由して受信した個々のIPパケット（IPSECパケット）は、上記処理部201にて上述したIPSEC処理が行われる。即ち、上記処理部201は、個々のIPSECパケットの上記AH、ESP情報を読み出し、上述した処理フローに従って上記一時データ記憶部202に格納された必要なSPD、SADを検索してIPSECに関する認証／暗号化、認証／復号化を行った後、送信先アドレスに送信する。また、その他の機能（ルーティング機能等）も上記処理部201にて提供される。

【0061】

ここで、個々のIPパケット処理時に、一時データ記憶部202に格納されたSPD、SADを検索する理由は、上記一時データ記憶部202がデータ記憶部203に比べて高速にアクセス可能であり、上記IPSEC処理の高速化を図ることができるためである。

【0062】

次に、図1、図3を用いて本実施の形態1におけるデータベース管理装置101の処理の詳細について説明する。

【0063】

データベース管理装置101を構成するSAD制御手段104は、有効期間におけるSAの削除、交換、更新開始時間における挿入、検索およびその要素の設定などを行うが詳細は後述する。尚、上記処理はその一例を示したのみであり、その他の処理を行っても構わない。

【0064】

また、SAD内の各SA（図1のSA1～SA5）の要素（必要事項）としては、送信ホストアドレス112、受信ホストアドレス113、プロトコル114、SPI115、登録時刻116、有効期間117、更新待ち期間118、関連SPI有無情報119、関連SPI120および相互参照情報121がある。な

お、前記 S A の要素はその一例を示したが、その他、従来技術にて示した認証アルゴリズム 1 2 1 2、認証鍵 1 2 1 3、暗号化アルゴリズム 1 2 1 4、暗号化鍵 1 2 1 5 等の情報を有していても構わなし、先に挙げた要素の中で不要なものは持たなくても構わない。

【 0 0 6 5 】

以上が本実施の 1 形態で取り扱う S A D システム 1 0 3 の基本構成である。

【 0 0 6 6 】

以降、本実施の形態 1 を、S A 1 (1 1 1) が有効期間の終了に達し、S A 5 1 3 1 が S A 1 (1 1 1) の有効期間後の S A となる場合を用いて説明を行う。尚、上記 S A D 内の各 S A の検索順序は、例えば各 S A が作成された順序や、当該 S A が記憶されている記憶領域のアドレス順に従って決定されるものである。又、本実施の形態 1 においては、上記有効期間の終了の管理については特に問題とならないため省略する。

【 0 0 6 7 】

まず、上記データベース管理装置 1 0 1 は、S A 1 (1 1 1) の有効期間が終了し、又は終了近くなると上記 S A 1 (1 1 1) の後継 S A となる S A 5 (1 3 1) を作成する。尚、当該 S A 5 (1 3 1) は、上述した I K E プロトコルを用いて相手側の通信端末と通信を行うことにより、当該 S A 5 に格納する必要事項を決定した後作成される。ここで、上記データベース管理装置 1 0 1 を構成する関連情報追加手段 1 0 5 は、当該 S A 1 (1 1 1) に、関連 S P I 有無情報 1 1 9、関連 S P I 1 2 0、相互参照情報 1 2 1 を追加する。

【 0 0 6 8 】

上記関連 S P I 有無情報 1 1 9 には、関連する（即ち後継 S A である）S A 5 (1 3 1) の存在の有無、即ち後述する関連 S P I 1 2 0 及び相互参照情報 1 2 1 の”有効”、”無効”を示すフラグが格納される。上記 S A 5 (1 3 1) が作成されるまでは当該関連 S P I 有無情報 1 1 9 には”無効”を示す情報が格納されることになる。又、上記関連 S P I 1 2 0 には、S A 5 (1 3 1) にて格納されている S P I 1 3 5 が、相互参照情報 1 2 1 には上記 S A 5 の場所情報、即ち、S A 5 が格納される領域のアドレスを示すポインタが格納される。

【0069】

さらに、SA5(131)において、関連SPI有無情報139には、関連するSA1(111)の存在の有無、即ち関連SPI140及び相互参照情報141の”有効”、”無効”を示すフラグが格納される。又、上記関連SPI140には、SA1(111)にて格納されているSPI115が、相互参照情報141には上記SA1(111)のアドレスを示すポインタが格納される。

【0070】

以上の関連SPI有無情報119、139、関連SPI120、140、相互参照情報121、141により、例えばSA1(111)がSAD制御手段104にて検索された場合にはSA5(131)の位置を、又、SA5(131)が検索された場合にはSA1(111)の位置を直ちに読み出すことが可能になる。

【0071】

続いて、図1、図3を用いて上記データベース管理装置101が、上記SAD102内のSAを検索する手順について説明する。

【0072】

上記SAD制御部104は、パケットの送受信時に、必要に応じてSAD102内のSAを順次検索し、目的とするSAを見つけるとその内容を読み出す。ここでは、例えばSA5(131)を適用したIPSECパケットが入力された場合の、SA5(131)の読み出しまでの例を説明する。

【0073】

まず前記IPSECのヘッダ情報より、受信ホストアドレス、プロトコルおよびSPIを検索条件として抽出する。次に、SAD内の全SAを検索したかを確認し、もし全SAの検索が終了している場合には検索を誤終了する(図3:S301YES→S309)。

【0074】

上記全SAを検索したかを確認する処理において、まだ検索していないSAがある場合には次の処理を行う(図3:S301NO→S302)。ここでは最初の検索であるために、次の処理を行う。

【0075】

続いて、上記抽出した受信ホストアドレス、プロトコルと、SA1内の受信ホストアドレス113、プロトコル114とを比較する（図3：S302）。

【0076】

尚、上記抽出した受信ホストアドレス、プロトコルと、SA1内の受信ホストアドレス113、プロトコル114が一致しなければ次のSAに検索処理を移す（図3：S302NO→S308→S301）。

【0077】

ここで、上記抽出した受信ホストアドレス、プロトコルと、SA1内の受信ホストアドレス113、プロトコル114が一致する場合、さらに上記抽出したSPIとSA1（111）のSPI115を比較する（図3：S302YES→S303）。

【0078】

上記抽出したSPIとSA1（111）のSPI115が等しい場合、当該IPSECパッケージが目的とするSAであるために、当該SAの内容を読み出して検索終了となる（図3：S303YES→S305）。

【0079】

尚、ここでは、SA5（131）が検索対象であるために、上記抽出したSPIはSPI115と一致しない。従って、次に関連SPI有無情報119の内容を確認する（図3：S303NO→S304）。

【0080】

続いて、上記関連SPI有無情報119が関連SPIの存在を示していない、即ち内容が“無効”である場合、次のSAに検索処理を移す（図3：S304NO→S308→S301）。上記“無効”は、後継SAが無いことを示し、これは通常通信時であって、未だSA1（111）が十分な有効期間を有する場合を示す。

【0081】

ここで、上記関連SPI有無情報119が関連SPIの存在を示している、即ち内容が“有効”である場合、上記抽出したSPIとSA1（111）の関連S

P I 1 2 0 とを比較する（図 3：S 3 0 4 Y E S → S 3 0 6）。

【0082】

上記抽出した S P I と S A 1（1 1 1）の関連 S P I 1 2 0 が異なる場合、当該 S A 1（1 1 1）は S A 5（1 3 1）とは関連しないとして、次の S A に検索処理を移す（図 3：S 3 0 6 N O → S 3 0 8 → S 3 0 1）。

【0083】

ここで、上記抽出した S P I と S A 1（1 1 1）の関連 S P I 1 2 0 が等しい場合、当該 S A 1（1 1 1）は後継 S A を有し、当該後継 S A の参照情報が相互参照情報 1 2 1 に格納されていることを意味するので、当該相互参照情報 1 2 1 に格納されている参照情報（ポインタ）を用いて S A 5（1 3 1）を決定する（図 3：S 3 0 6 Y E S → S 3 0 7）。続いて、上記 S A 5（1 3 1）が格納する必要事項より構成される情報を読み出して、検索は正常終了となる（図 3：S 3 0 7 → 検索正常終了）。

【0084】

以上の処理にて読み出された各 S A に格納される必要事項が、当該 I P S E C パケットの暗号化の解除（復号化）等にご利用されるのは従来技術と同様である。尚、上記関連 S P I 有無情報、関連 S P I、相互参照情報を参照する処理（S 3 0 4、S 3 0 6、S 3 0 7）は、上記 S A D 制御手段 1 0 4 を構成する関連情報検索手段 1 0 6 にて行われる。

【0085】

以上のように、従来では S A 1 が検索対象でない場合には、例えば S A 2、S A 3 といった順に検索を行う必要があったが、関連 S P I 有無情報、関連 S P I、相互参照情報といったデータ間の関連情報をそれぞれのデータに設けることにより、一方のデータが検索された場合に、関連する他方のデータを瞬時に読み出すことが可能になる。これにより、目的とする S A を検索する速度を高めるとともに、データベース管理装置の負荷を下げるができる。

【0086】

尚、本実施の形態 1 では、S A の関連情報を上記関連 S P I 有無情報、関連 S P I、相互参照情報の 3 つにしたが、その他の情報を有していても構わなし、不

要なものは必ずしも必要ない。又、本実施の形態では S A から関連する S A への参照方法に格納領域のアドレス（ポインタ）を用いたが、データベースが管理するデータのエントリ番号等を用いても構わない。

【 0 0 8 7 】

又、上記 S A の検索手順では、 S P I 以外の検索条件に受信ホストアドレス、プロトコルを用いたが、これらに加えてパケットの優先処理フラグ（ I P v 4 では " Type of Service " フィールド、 I P v 6 では " Flow Label " フィールド）を検索条件に加えても構わないし、必要な場合にはその他の情報を検索条件に加えてもよい。

【 0 0 8 8 】

〔実施の形態 2〕

次に、図 4、図 5 を用いて本実施の形態 2 におけるデータベース管理装置 4 0 1 の構成を説明する。尚、上記データベース管理装置 4 0 1 は上記実施の形態 1 と共通点が多いため、異なる点のみ説明する。又、 S A D 1 0 2 に記憶される各 S A （ここでは S A 1 ～ S A 5 ）には、登録時刻 1 1 6、1 3 6、有効期間 1 1 7、1 3 7、更新待ち期間 1 1 8、1 3 8 がそれぞれ格納されるが、例えば上記実施の形態 1 にて説明した関連 S P I 有無情報、関連 S P I、相互参照情報等の関連情報は必ずしも必要ではない。また、更新待ち時間 1 1 8、1 3 8 も必ずしも必要ではない。ここで、上記 S A 1 （1 1 1）の登録時刻 1 1 6 には、図 5 に示す、当該 S A 1 （1 1 1）が作成された登録時刻 5 0 1 の値が格納される。又、上記有効期間 1 1 7 には当該 S A 1 （1 1 1）が通信において使用可能な有効期間 5 0 2 が格納される。さらに、更新待ち期間 1 1 8 には、上述した I K E プロトコルを用いた後継 S A の作成に必要な時間 5 0 5 にある程度余裕を持たせた時間（図 5 に示す更新待ち期間 5 0 3）が格納される。但し、上記登録時刻 1 1 6、有効期間 1 1 7、更新待ち期間 1 1 8 は、上記図 5 における登録時刻 5 0 1、有効期間終了時刻 5 0 5、及び更新開始時刻 5 0 6 を特定できるものであればよく、時刻や時間、その他の異なる型式の情報として格納してもよい。ここに更新開始時刻とは、例えば上記 I K E プロトコルを用いた通信を開始する時刻である。

【 0 0 8 9 】

本実施の形態 2 におけるデータベース管理装置 4 0 1 は、さらに有効期間管理手段 4 0 2 を備える。当該有効期間管理手段 4 0 2 には、各 S A 1 ～ 5 に対応する有効期間管理情報 4 1 0 ～ 4 1 4 が格納される。当該有効期間管理情報 4 1 0 ～ 4 1 4 には、対応する S A 1 ～ 5 の位置情報（ポインタ）が参照情報として、又、対応する S A 1 ～ 5 の有効期間終了時刻（例えば図 5 の 5 0 5）が有効期間終了時刻として格納される。尚、上記有効期間管理情報は、当該 S A の登録時に当該有効期間管理手段 4 0 2 により登録される。上記有効期間管理情報 4 1 0 ～ 4 1 4 は、イベントキューの形で格納されており、有効期間終了時刻の早い順に並んでいるものとする。尚、上記参照情報はポインタに限らず、データベースにおけるエントリ番号等、上記 S A 1 ～ 5 を特定して参照可能な情報であればよい。

【 0 0 9 0 】

続いて図 4 を用いて、上記有効期間管理手段 4 0 2 の処理の詳細を説明する。

【 0 0 9 1 】

上記有効期間管理手段 4 0 2 を構成するイベント起動部 4 0 3 は、S A 1 が作成された旨を示す情報を S A D 制御手段 4 0 5 から受け取ると、当該 S A 1 に対応する有効期間管理情報 4 1 0 を有効期間管理手段 4 0 2 内に格納する。有効期間管理情報の内容は上述した通りであるが、有効期間終了時刻は当該登録時点において S A 1 内に格納されている登録時刻 1 1 6 及び有効期間 1 1 7 を用いて算出される。以後、同様に順次 S A 2 ～ S A 4 に関しても有効期間管理情報 4 1 1 ～ 4 1 3 が格納される。

【 0 0 9 2 】

続いて、上記有効期間管理情報 4 1 0 が格納されると、当該有効期間管理情報 4 1 0 を構成する有効期間終了時刻は、イベント起動部にて読み込まれ、該イベント起動部 4 0 3 は上記有効期間終了情報を計時部 4 0 4 に設定する。

【 0 0 9 3 】

上記計時部 4 0 4 は、常時時刻を監視し、上記 S A 1 に対応する有効期間終了時刻が来ると上記イベント起動部 4 0 3 に通知する。

【 0 0 9 4 】

上記通知を受けると、イベント起動部 4 0 3 は上記有効期間管理情報 4 1 0 を参照し、S A 1 の参照情報を読み出して S A D 制御手段 4 0 5 に当該参照情報を送信すると共に、続く S A 2 に対応する有効期間管理情報 4 1 1 について計時部 4 0 4 への設定を行う。

【 0 0 9 5 】

上記参照情報を受信した S A D 制御手段 4 0 5 は、当該参照情報に基づいて S A 1 を削除する。又、同時に S A 1 に対応する後継 S A である、S A 5 の作成、登録処理を行ってもよい。

【 0 0 9 6 】

以上のように、従来では、所定の時刻に当該 S A に関するパケットの入出力が無い場合には当該 S A に対して作成、登録や削除処理等が行われたかったが、S A の有効期間を管理するための機能を付加することで、S A の作成、登録や削除等、必要な処理を確実に行うことができる。上記必要な処理を確実に行うことにより、不要な S A を放置することによる検索速度の低下や S A D の記憶領域の無駄を防ぐことが可能となる。

【 0 0 9 7 】

尚、上記実施の形態 1 にて説明した関連情報を上記実施の形態 2 における各 S A に追加するとともに、S A D 制御手段 1 0 4 を構成する関連情報検索手段 1 0 6、関連情報追加手段 1 0 5 を上記 S A D 制御手段 4 0 5 に採用することにより、S A の検索速度をより一層高速化することが可能となる。

【 0 0 9 8 】

〔実施の形態 3〕

次に、図 5、図 6 を用いて本実施の形態 3 におけるデータベース管理装置 6 0 1 について説明する。尚、本実施の形態 3 におけるデータベース管理装置 6 0 1 は上記実施の形態 2 と共通点が多いため、異なる点のみ説明する。又、S A D 1 0 2 に記憶される各 S A（ここでは S A 1 ～ S A 5）には、登録時刻 1 1 6、1 3 6、有効期間 1 1 7、1 3 7、更新待ち期間 1 1 8、1 3 8 がそれぞれ格納されるが、例えば上記実施の形態 1、2 にて説明した関連 S P I 有無情報、関連 S

P I、相互参照情報等の関連情報は必ずしも必要ではない。

【 0 0 9 9 】

本実施の形態 3 におけるデータベース管理装置 6 0 1 は、上記実施の形態 2 にて説明した有効期間管理手段 4 0 2 を備える。但し、当該有効期間管理手段 4 0 2 には、有効期間管理情報 4 1 0 ～ 4 1 4 に加えて、更新開始時刻情報 6 1 1 ～ 6 1 3 が格納される。当該更新開始時刻情報 6 1 1 ～ 6 1 3 には、対応する S A 1 ～ 5 の位置情報（ポインタ）が参照情報として、又、対応する S A 1 ～ 5 の更新開始時刻（例えば図 5 の 5 0 6）が更新開始時刻として格納される。尚、上記情報は、当該 S A の登録時に当該有効期間管理手段 4 0 2 により登録される。上記更新開始時刻情報 6 1 1 ～ 6 1 3 も、イベントキューの形で格納されており、更新開始時刻、及び有効期間終了時刻の早い順に並んでいるものとする。即ち、通常、例えば S A 1 に関する更新開始時刻情報 6 1 1 の次に S A 1 に関する有効期間管理情報が格納される。

【 0 1 0 0 】

続いて図 6 を用いて、上記有効期間管理手段 4 0 2 の処理の詳細を説明する。

【 0 1 0 1 】

上記有効期間管理手段 4 0 2 を構成するイベント起動部 4 0 3 は、S A 1 が作成された旨を示す情報を S A D 制御手段 4 0 5 から受け取ると、当該 S A 1 に対応する更新開始時刻情報 6 1 1 を有効期間管理手段 4 0 2 内に格納し、続いて有効期間管理情報 4 1 0 を有効期間管理手段 4 0 2 内に格納する。

【 0 1 0 2 】

更新開始時刻は当該登録時点において S A 1 内に格納されている登録時刻 1 1 6、有効期間 1 1 7、及び更新待ち期間 1 1 8 を用いて算出される。以後、同様に順次 S A 2 ～ S A 4 に関しても更新開始時刻情報 6 1 1 ～ 6 1 3、及び有効期間管理情報 4 1 1 ～ 4 1 3 が格納される。

【 0 1 0 3 】

続いて、上記更新開始時刻情報 6 1 1 が格納されると、当該更新開始時刻情報 6 1 1 を構成する更新開始時刻は、イベント起動部にて読み込まれ、該イベント起動部 4 0 3 は上記更新開始時刻を計時部 4 0 4 に設定する。

【 0 1 0 4 】

上記計時部 4 0 4 は、常時時刻を監視し、上記 S A 1 に対応する更新開始時刻が来ると上記イベント起動部 4 0 3 に通知する。

【 0 1 0 5 】

上記通知を受けると、イベント起動部 4 0 3 は上記更新開始時刻情報 6 1 1 を参照し、S A 1 の参照情報を読み出して S A D 制御手段 4 0 5 に当該参照情報を送信すると共に、続く有効期間管理情報 4 1 0 について計時部 4 0 4 への設定を行う。尚、有効期間管理情報に対する有効期間管理手段の処理は上記実施の形態 2 にて示した通りである。

【 0 1 0 6 】

上記参照情報を受信した S A D 制御手段 4 0 5 は、当該参照情報に基づいて、S A 1 に対応する後継 S A である S A 5 を作成、登録するための I K E プロトコルを用いたネゴシエーションを行う。但し、当該ネゴシエーションは I P S E C 通信にて利用される他の手段が行ってもよい。この場合には、上記 S A D 制御手段 4 0 5 は、上記他の手段に当該 S A 1 の情報及び上記ネゴシエーションを行う旨の指示を送信する。

【 0 1 0 7 】

上記 S A D 制御手段 4 0 5 がネゴシエーションを行う場合を仮定すると、当該ネゴシエーション終了後 S A 5 が作成され、上記 S A D 制御手段 4 0 5 は当該 S A 5 (1 3 1) の登録時刻 1 3 6 に上記 S A 5 (1 3 1) を作成、登録した時刻を格納し、さらにあらかじめ決められている有効時間 1 3 7、更新待ち期間 1 3 8 も格納する。次に、当該作成した情報を上記有効期間管理手段 4 0 2 に通知し、当該有効期間管理手段 4 0 2 は、上記 S A 5 に関する更新開始時刻情報 6 1 3 を登録するに至る。

【 0 1 0 8 】

さらに、上記 S A D 制御手段 4 0 5 は、上記実施の形態 1 にて説明した関連情報、即ち関連 S P I 有無情報 1 1 9、1 3 9、関連 S P I 1 2 0、1 4 0、相互参照情報 1 2 1、1 4 1 にそれぞれ情報を格納する。又、同時に上記 S A 1 (1 1 1) と S A 5 (1 3 1) との検索順序を入れ換えてもよい。当該入れ替えの詳細

細は S A D の検索方法により異なるために割愛する。

【 0 1 0 9 】

続いて、有効期間管理情報 4 1 0 の格納する有効期間終了時刻がくると、上記有効期間管理手段 4 0 2 は、その旨を S A D 制御手段 4 0 5 に通知し、当該 S A D 制御手段 4 0 5 は上記有効期間管理情報 4 1 0 に格納されている参照情報を基に S A 1 (1 1 1) を削除する。又、当該削除に際して、関連する S A 5 (1 3 1) の関連 S P I 有無情報 1 3 9 を” 無効 ” に書き換えると共に、関連 S P I 1 4 0 及び相互参照情報 1 4 1 の内容を消去する。

【 0 1 1 0 】

以上のように、更新開始時刻 5 0 6 を正確に管理し、当該更新開始時刻には確実に I K E プロトコルを用いたネゴシエーションを行うことにより、上記 S A 1 に関するパケットが送受信されていない場合にも確実に後継 S A を作成、登録することが可能になる。また、更新待ち期間に十分な余裕を持たすことにより、S A 1 と後継 S A 5 の何れかが常時有効な状態で存在することになり、S A の作成、登録のための通信の遅延を確実に無くすることができる。

【 0 1 1 1 】

さらに、上記十分な時間の余裕により、後継 S A である S A 5 が生成、登録された後もしばらく S A 1 が存在するために、S A 1 を適用した I P S E C パケットがネットワークの遅延等により遅れて到着した場合にも、当該パケットを破棄することなく正常に処理することが可能となる。これは、特に長時間のリアルタイム映像を送受信する場合等に、全てのパケットを問題なく処理でき、しかも関連情報により後継 S A またはその元となる S A を瞬時に検索できるため、受信した映像にブランクや乱れを生じるにくくすることができる。

【 0 1 1 2 】

尚、上記後継 S A の作成に関する更新開始時刻情報 6 1 1 ~ 6 1 3 を、有効期間管理手段と同様の機能を有する更新管理手段によりまとめて処理するようにしてもよい。

【 0 1 1 3 】

〔実施の形態 4〕

次に、図 7 を用いて本実施の形態 4 におけるデータベース管理装置 7 0 1 について説明する。尚、本実施の形態 4 におけるデータベース管理装置 7 0 1 は上記実施の形態 1 ～ 3 と共通点が多いため、異なる点のみ説明する。

【 0 1 1 4 】

本実施の形態 4 では、S A D 制御手段 1 0 4 内に、有効期間延長手段 7 0 2 を備える。また当該有効期間延長手段 7 0 2 には、延長期間情報 7 0 3 が記憶されている。

【 0 1 1 5 】

S A 1 (1 1 1) が S A D 制御手段 1 0 4 にて検索されたにもかかわらず、上記 S A 1 (1 1 1) を構成する有効期間 1 1 7 の情報が、既に有効期間を過ぎたものであった場合、上記有効期間延長手段 7 0 2 は、上記有効期間 1 1 7 の情報に上記延長期間情報 7 0 3 を加えた値を暫定有効期間とし、当該暫定有効期間に基づいて S A 1 (1 1 1) の有効期間を判定する。

【 0 1 1 6 】

S A D 制御手段 1 0 4 にて検索された時刻が、上記暫定有効期間内であった場合、当該 S A 1 (1 1 1) を有効とし S A 1 を用いてパケットの符号化、復号化等を行う。

【 0 1 1 7 】

通常、有効期間の終了間際に、パケットが送信端末から出力された場合には、受信端にパケットが届く時間には S A の有効期間が終了しており、そのパケットは破棄されてしまうが、以上のように、有効期間延長手段を設けることで、本来破棄されるパケットを破棄することなく活用することができる。

【 0 1 1 8 】

尚、上記延長期間情報は、通信先となる端末とのネットワーク構成やトラフィックを考慮して、通信先毎に独立して設けることで、通信状況に応じた設定が可能となる。

【 0 1 1 9 】

〔実施の形態 5〕

次に、図 1、図 8 を用いて本実施の形態 5 におけるデータベース管理装置 8 0

1について説明する。尚、本実施の形態5におけるデータベース管理装置801は上記実施の形態1～4と共通点が多いため、異なる点のみ説明する。又、図1については、検索順序のみを参照する。

【0120】

本実施の形態5におけるデータベース管理装置801は、検索頻度監視手段802を備える。さらに、検索頻度監視手段802には、更新開始時刻が到来したSA1と、そのSAの有効期間終了後にそのSAの後継SAとなるSA5への参照情報を持っている。

【0121】

以降、上記SA1の更新開始時刻が到来した後で、かつSA1の有効期間が未だ終了しない間の状態、即ち図5における期間510の状態の場合の処理について説明する。尚、SA1(111)の後継SAがSA5(131)であるとする。

【0122】

まず、検索頻度監視手段802は、SA5(131)がSA1(111)と関連のあるSAであることを更新開始時刻の処理にて認識し、SA1の検索回数とSA5の検索回数の両方のカウントを開始する。次に、設定した所定の時間間隔で検索回数が多いSAを決定し、その後、参照情報810および811を用いて検索回数の多い順、例えばSA5(131)の検索順序を図1の検索順序から図8に示す検索順序に変更する。即ち、検索順が、「SA1→SA2→SA3→SA4→SA5」であったのを「SA5→SA2→SA3→SA4→SA1」に変更する。尚、当該検索順序の変更の詳細はSADの検索方法により異なるために割愛する。

【0123】

なお、本実施の形態5では、検索回数が多いSAを早い検索順序に設定したが、SA1の有効期間後のSAであるSA5を検索回数に関係なく、早い検索順序に設定しても構わない。

【0124】

以上により、後継SA(SA5)と当該後継SAに対応するSAがどちらも検

索される期間において、2つのSAのうち検索頻度が高いSAを検索時間の短い検索順序に設定することで、検索頻度の高いSAを短時間で検索することが可能になる。

【図面の簡単な説明】

【図1】

本発明に係るデータベース管理装置及びSADの概略を示すイメージ図。

【図2】

本発明に係るデータベース管理装置を格納するネットワーク接続装置のハードウェアブロック図。

【図3】

本発明に係るデータベース管理装置の処理を示すフローチャート。

【図4】

実施の形態2におけるデータベース管理装置及びSADの概略を示すイメージ図。

【図5】

時間軸に対応するSAの状況を示す図。

【図6】

実施の形態3におけるデータベース管理装置及びSADの概略を示すイメージ図。

【図7】

実施の形態4におけるデータベース管理装置及びSADの概略を示すイメージ図。

【図8】

実施の形態5におけるデータベース管理装置及びSADの概略を示すイメージ図。

【図9】

従来のIPSEC機能を搭載したルータを使用したネットワークシステムの概略図。

【図10】

I P S E C 機能を搭載したネットワーク接続装置間での接続手順を表した図。

【図 1 1】

従来技術における S P D (Security Policy Database) の一例。

【図 1 2】

従来技術における S A D (Security Association Database) の一例。

【図 1 3】

送信側ネットワーク接続装置における I P S E C 処理のフローチャート。

【図 1 4】

受信側ネットワーク接続装置における I P S E C 処理のフローチャート。

【図 1 5】

時間軸に対応する S A の状況を説明するイメージ図。

【符号の説明】

1 0 1 - データベース管理装置

1 0 2 - セキュリティアソシエーションデータベース

1 0 3 - S A D システム

1 0 4 - S A D 制御手段

1 0 5 - 関連情報追加手段

1 0 6 - 関連情報検索手段

1 1 1、1 3 1 - S A

1 1 2、1 3 2 - 送信ホストアドレス

1 1 3、1 3 3 - 受信ホストアドレス

1 1 4、1 3 4 - プロトコル

1 1 5、1 3 5 - S P I

1 1 6、1 3 6 - 登録時刻

1 1 7、1 3 7 - 有効期間

1 1 8、1 3 8 - 更新待ち時間

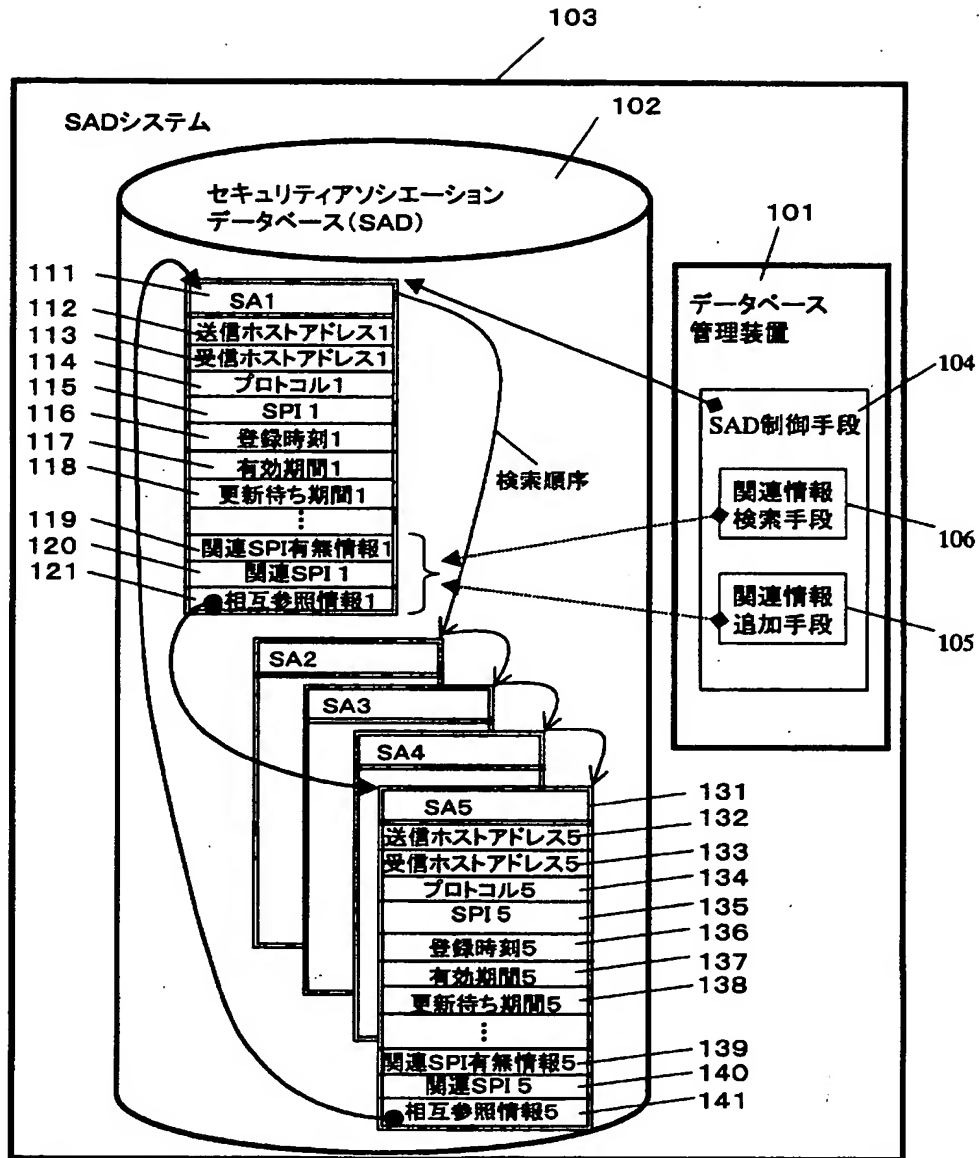
1 1 9、1 3 9 - 関連 S P I 有無情報

1 2 0、1 4 0 - 関連 S P I

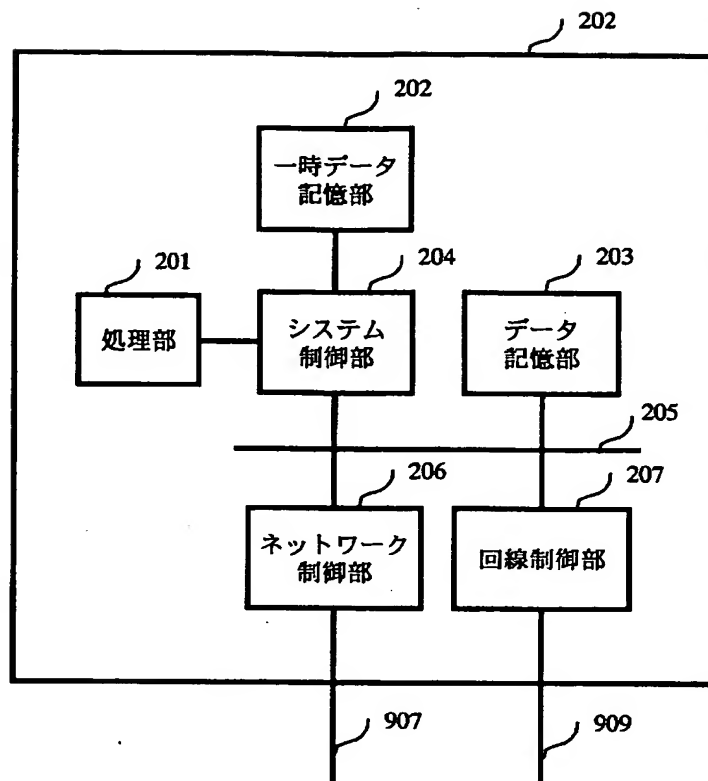
1 2 1、1 4 1 - 相互参照情報

【書類名】 図面

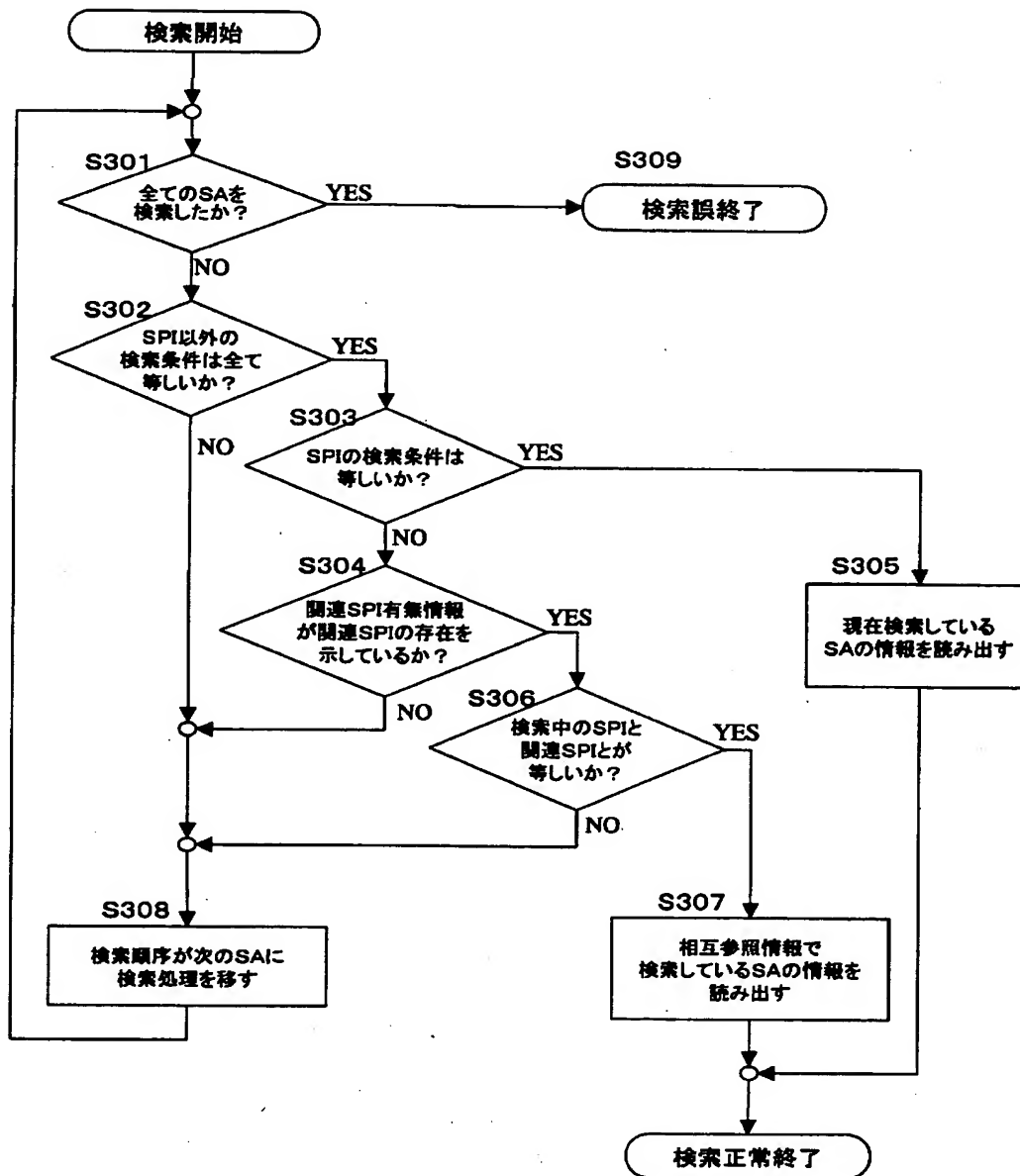
【図 1】



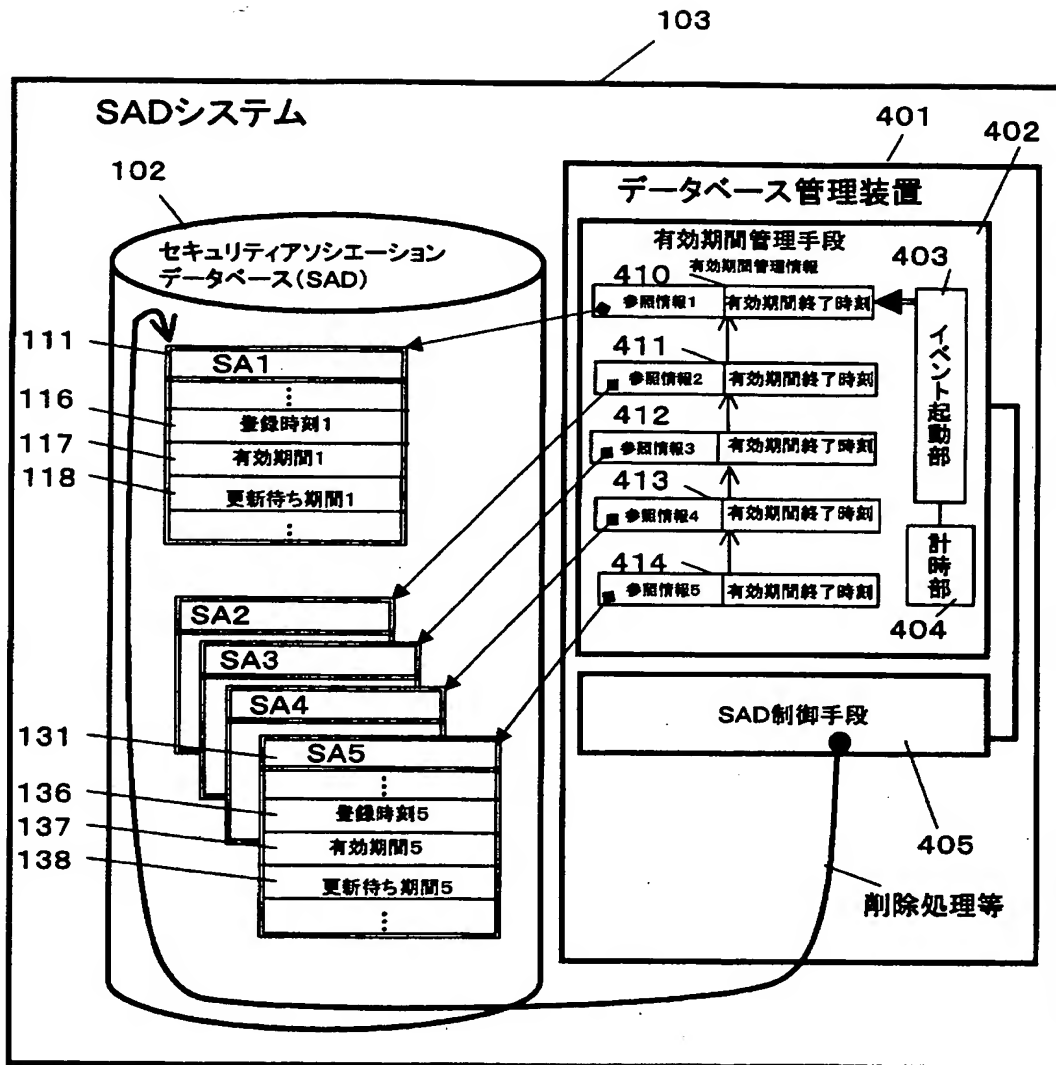
【図 2】



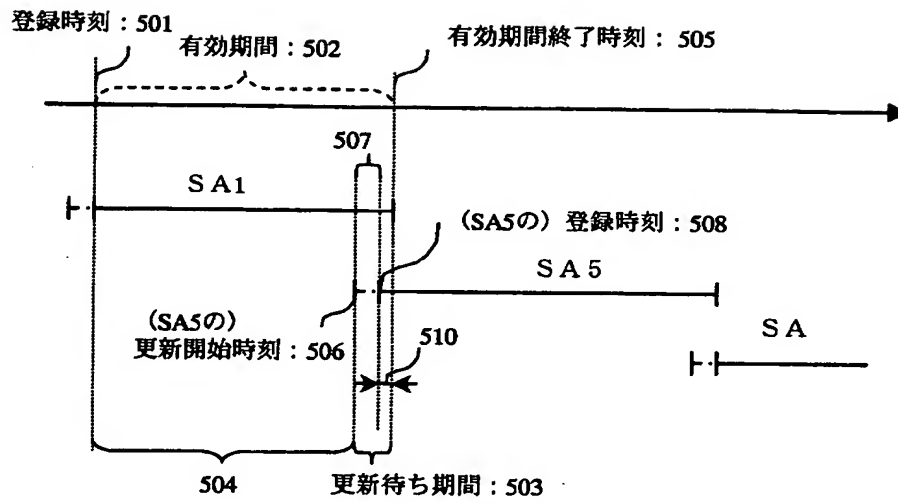
【図 3】



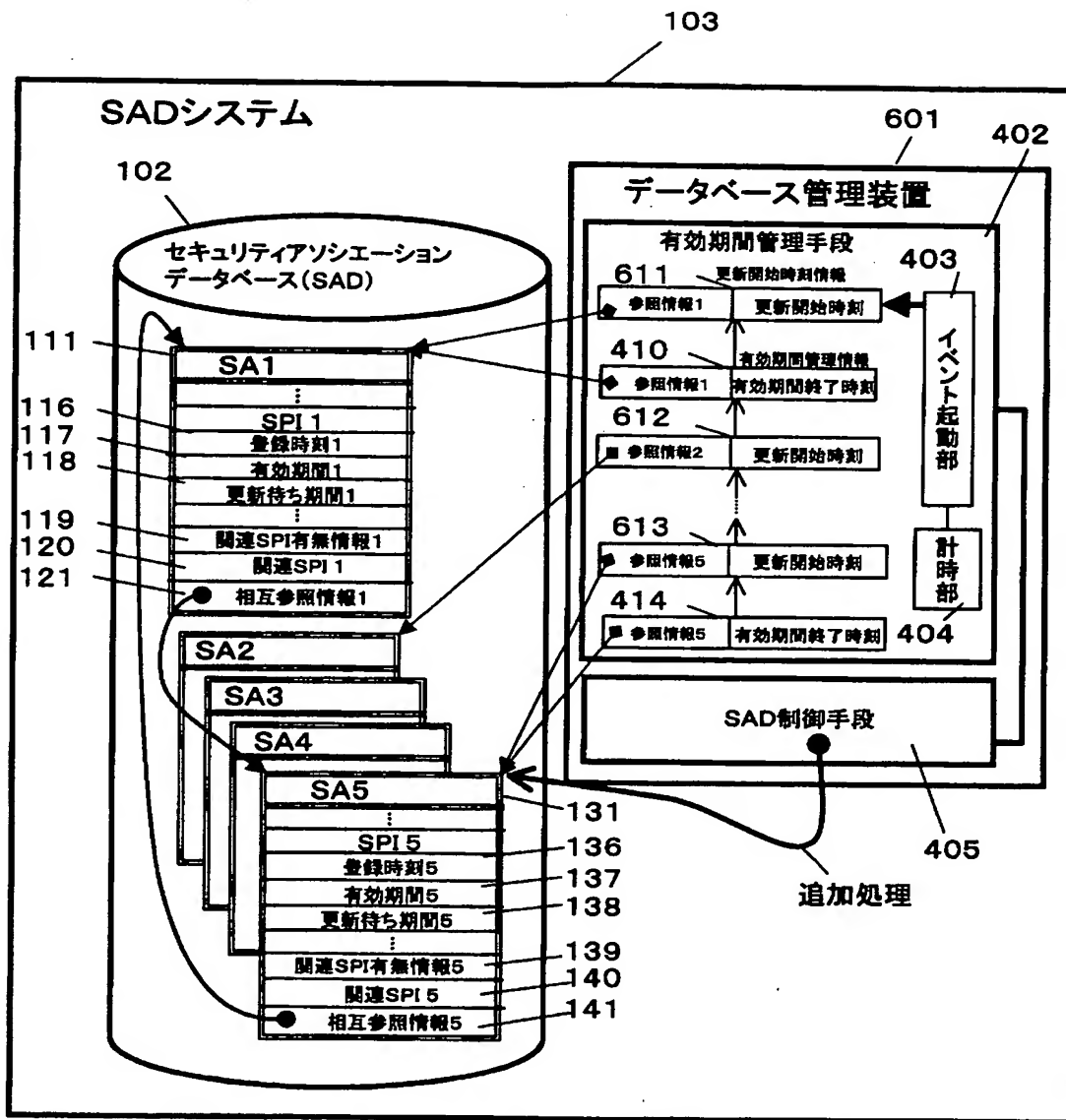
【図 4】



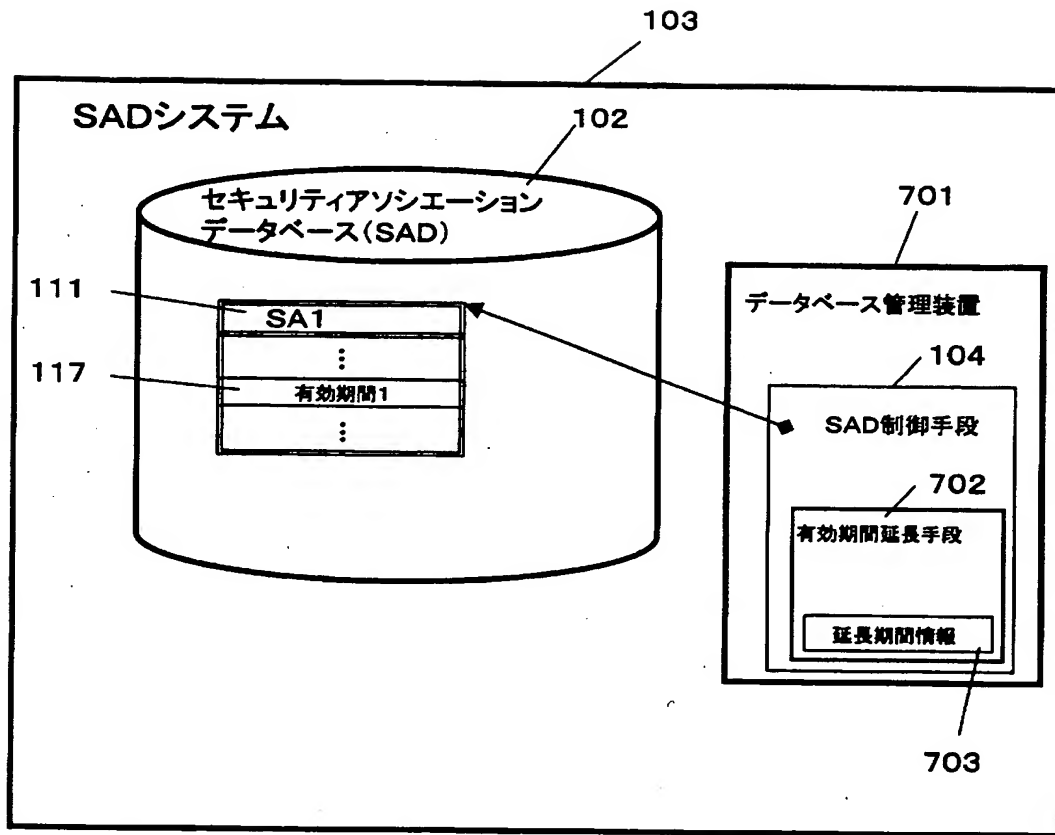
【図 5】



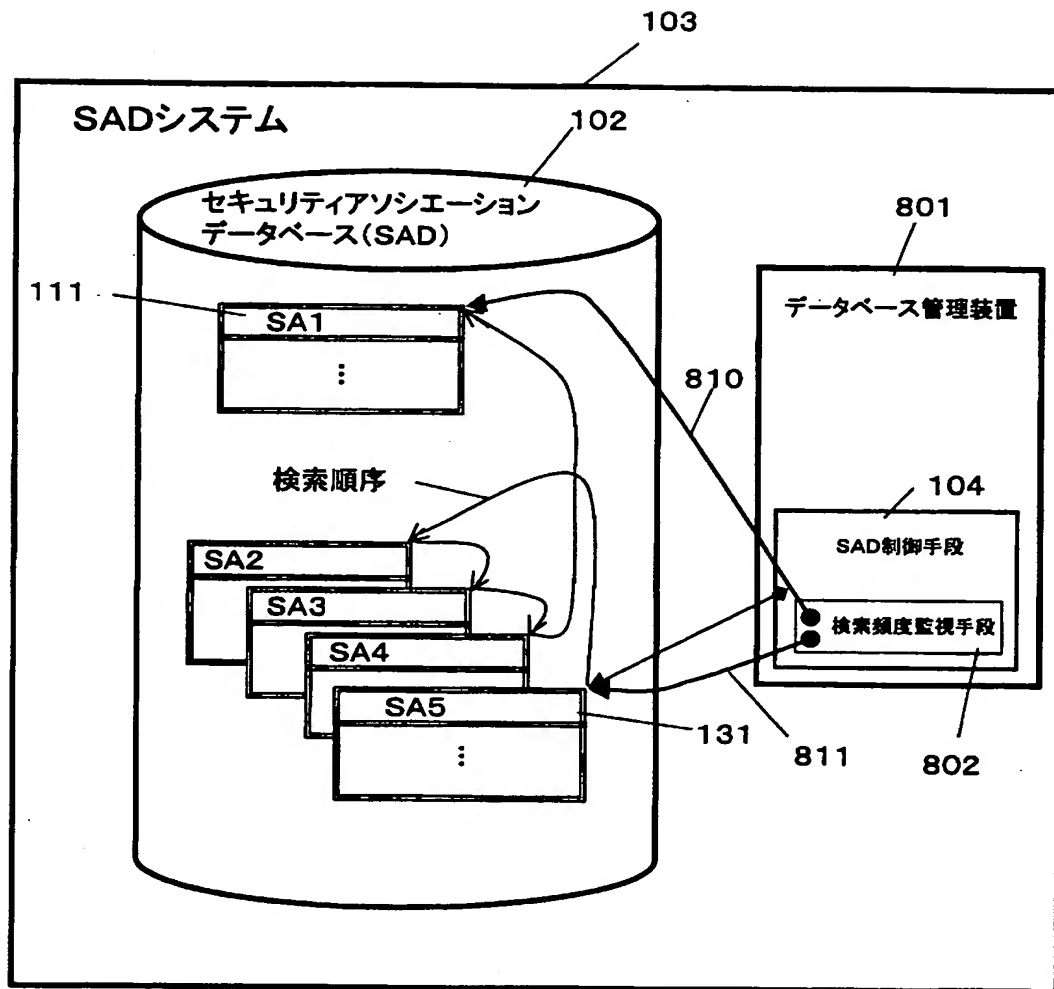
【図 6】



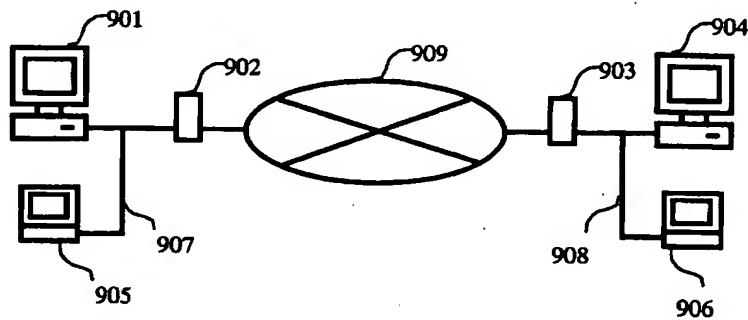
【図 7】



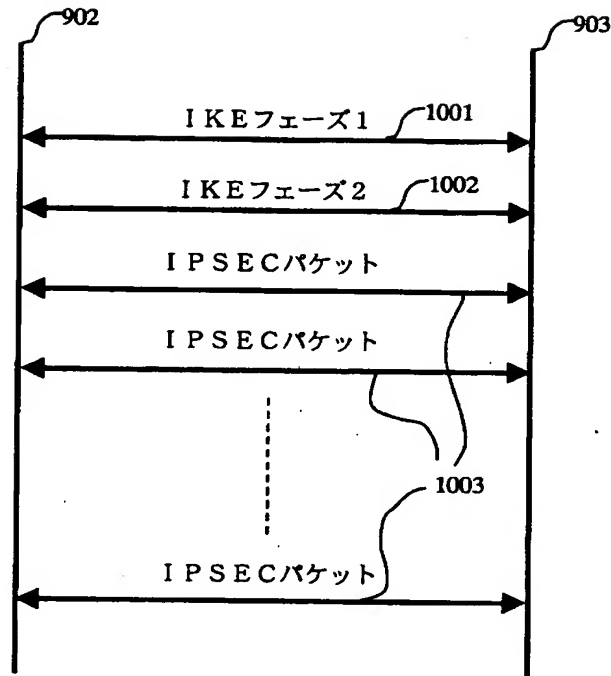
【図 8】



【図 9】



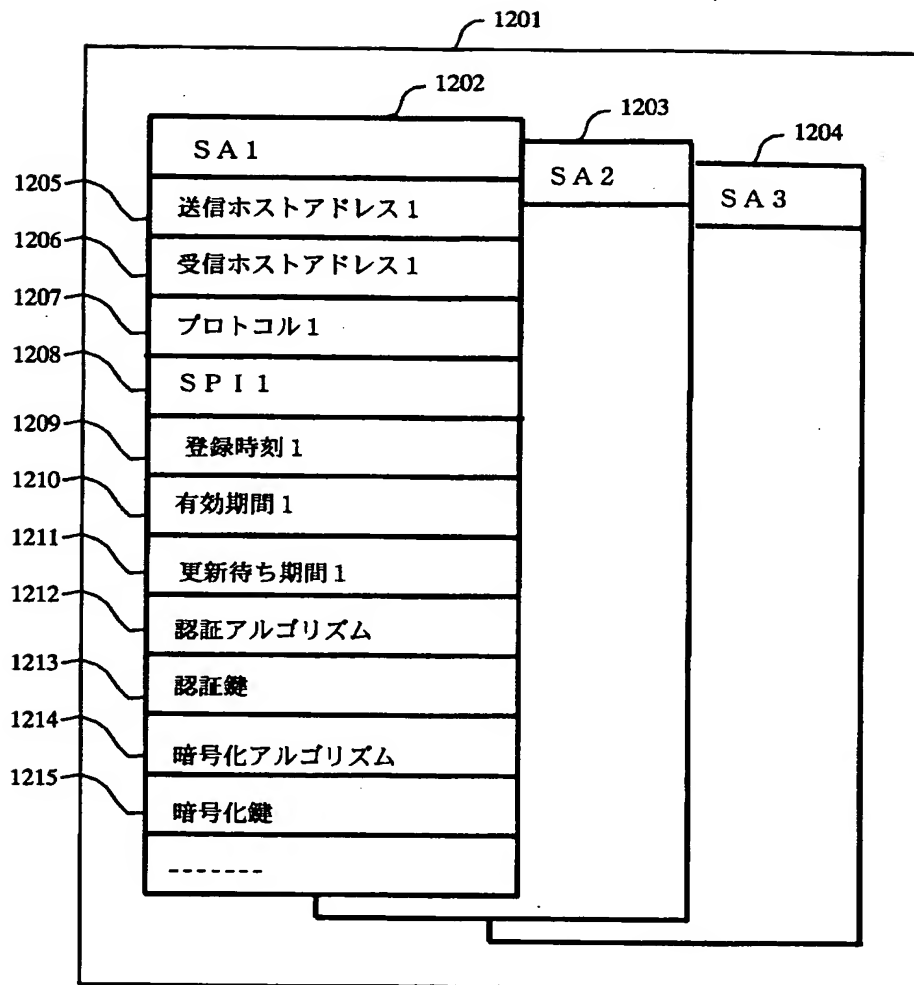
【図10】



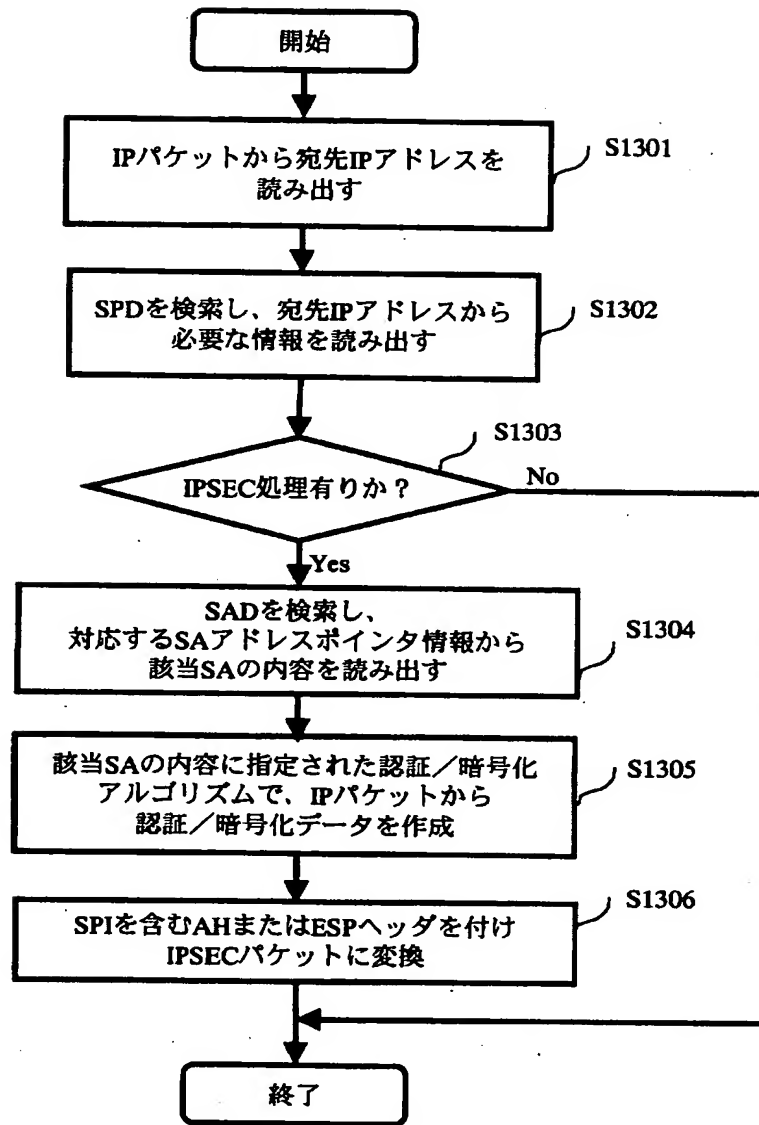
【図11】

IPA-1	IPSEC-IPA-1	有	SA1
IPA-2	IPSEC-IPA-2	無	—
IPA-3	IPSEC-IPA-3	有	SA3
-----	-----	-----	-----
IPA-L	IPSEC-IPA-L	有	SAM

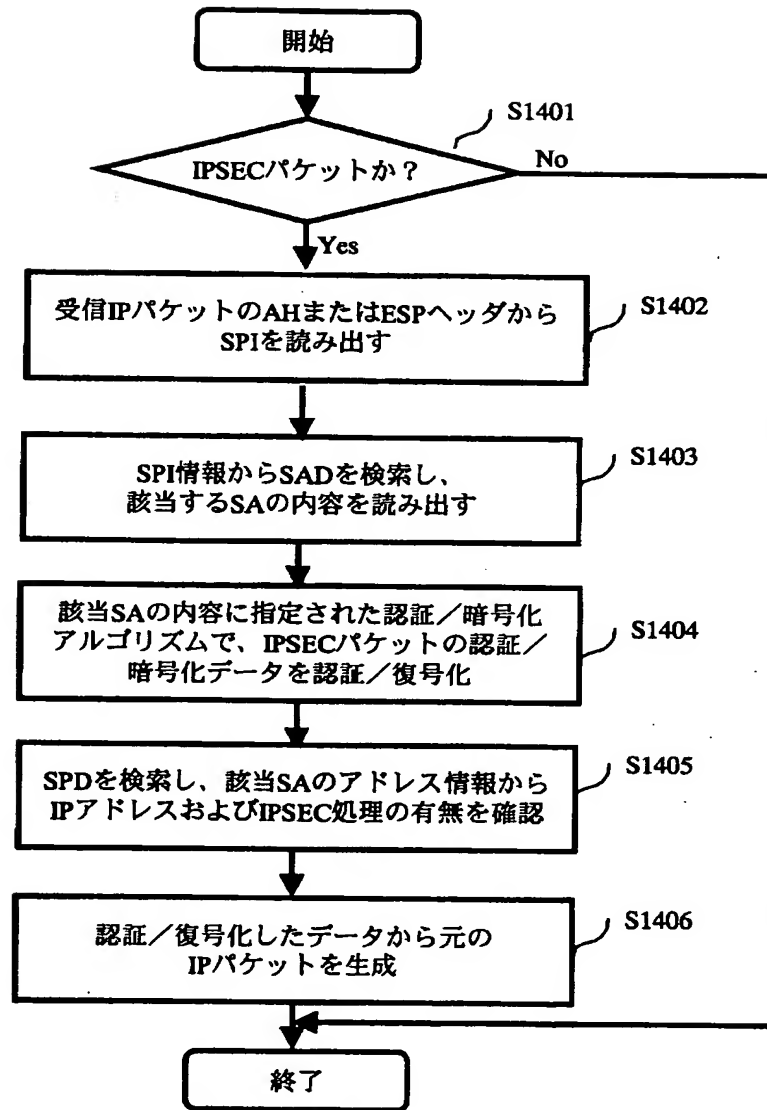
【図 1 2】



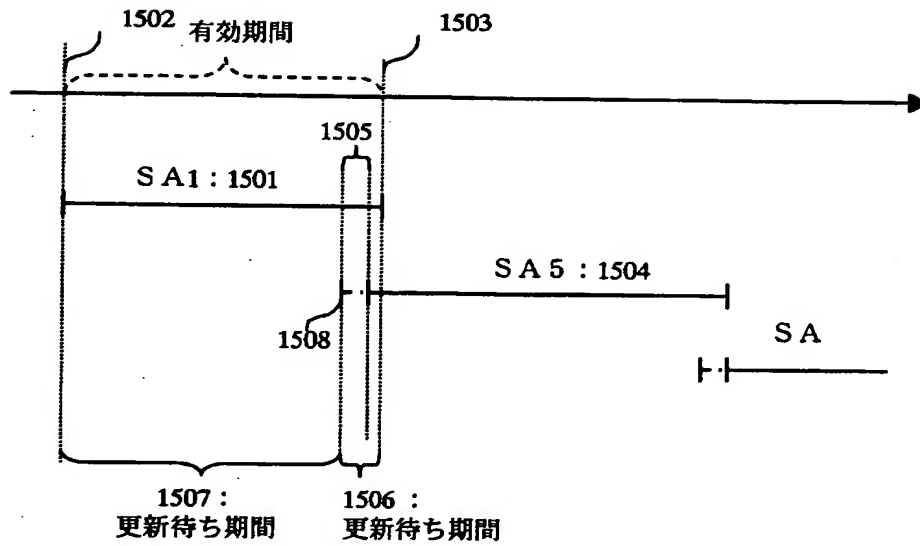
【図13】



【図 1 4】



【図 1 5】



【書類名】 要約書

【要約】

【課題】 データベース内の検索対象となるデータを短時間に検索すると共に、有効期間の終了するデータと当該データの後継データとの切換をスムーズに行うデータベース管理装置、管理方法及びその記録媒体を提供する。

【解決手段】 有効期間が終了する所定のデータと、当該所定のデータに対応する後継データとの両方又はどちらか一方に上記データを相互に関連付けた関連情報を追加する関連情報追加手段を具備するデータベース管理装置、管理方法及び記録媒体を提供する。

【選択図】 図 1

特 2000-392661

出 願 人 履 歴 情 報

識別番号 [000005821]

1. 変更年月日	1990年 8月28日
[変更理由]	新規登録
住 所	大阪府門真市大字門真1006番地
氏 名	松下電器産業株式会社